UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/816,335	03/31/2004	Tim Harmon	US03 0022	8799

7590 02/07/2007

PHILIPS ELECTRONICS NORTH AMERICA CORPORATION
Intellectual Property & Standards
345 Scarborough Road
Briarcliff Manor, NY 10510

EXAMINER	
ALPHONSE, FRITZ	
ART UNIT	**PAPER NUMBER**
2133	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/816,335	HARMON, TIM	
	Examiner	Art Unit	
	Fritz Alphonse	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pomet (U.S. Pat. 6,230,178) in view of Monier (U.S. Pat. No. 5,745,398).

As to claims 17 and 28, Pomet (fig. 2) discloses a circuit arrangement, comprising: a working register (201); an error correction parameter circuit configured to determine an error correction parameter for use in Montgomery modular processing by performing a modulo operation on a modulus value (col. 2, lines 25-40), wherein the error correction parameter circuit is configured to perform the modulo operation by sequentially performing a plurality of shift/compare operations on contents of the working register (col. 3, lines 40-55).

Pomet does not explicitly disclose the error correction parameter circuit is further configured to store an initial value in the working register that is greater than the modulus value.

However, in the same field of endeavor, Monier discloses a method for the implementation of modular multiplication wherein an error correction parameter circuit is configured to store an initial value in the register that is greater than the modulus value (col. 10, lines 11-20).

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention to improve upon the method for the implementation of modular multiplication,

as disclosed by Monier. Doing so would improve the implementation of the modular multiplication in order to reduce the periods of time needed for this multiplication to take place.

As to claims 18-20, Pomet (fig. 2) discloses a circuit arrangement, wherein the initial value correlates to a working register value of one position past a most significant bit of the modulus value (col. 3, lines 40-55); the error correction parameter circuit further comprises a state machine (202) configured to determine a most significant bit of the modulus value; the state machine checks each word of the modulus value for the most significant bit (col. 4, lines 39-50).

As to claims 21-24, Pomet discloses a circuit arrangement, wherein the error correction parameter circuit further comprises a variable shifter configured to left shift the working register to produce a shifted result (col. 3, lines 40-55); the error correction parameter circuit further comprises a subtraction circuit configured to process the modulus value and the shifted result using bit-by-bit subtraction to determine a subtracted result (col. 3, lines 55-67); the error correction parameter circuit further comprises a plurality of registers (201, 202) for separately storing the shifted and subtracted results.

As to claims 25-27 and 29-31, Pomet (fig. 2) discloses a circuit arrangement, wherein the error correction parameter circuit further comprises a variable shifter configured to shift the working register a plurality of spaces in a single loop iteration (col. 5, lines 53-67); the program product comprising hardware definition program code; and, wherein the plurality of shift/compare operations include a shift function and a subtraction function executed in parallel(col. 3, lines 22-31).

As to claims 1 and 13, Pomet (fig. 2) discloses a method of determining an error correction parameter for use in Montgomery modular processing, comprising: performing a modulo operation on a modulus value by sequentially performing a plurality of shift/compare operations on contents of a working register (col. 2, lines 25-52).

Pomet does not explicitly disclose the error correction parameter circuit is further configured to store an initial value in the working register that is greater than the modulus value. However, the limitation is obvious and well known in the art, as evidenced by Monier (col. 10, lines 11-20). See the motivation for the same reason disclosed in claims 17 and 28 above.

As to claims 2-6, 14-16, Pomet (fig. 2) discloses a method comprising determining the initial value by left shifting the contents of the working register a number of positions correlating to one position past a most significant bit of the modulus value; checking each word of the modulus value for the most significant bit; determining the initial value while the modulus value loads (col. 2, lines 25-52). Pomet (fig. 2) discloses a method, wherein the plurality of shift/compare operations further comprises left shifting the working register to determine a shifted result.

As to claims 7-9, Pomet (fig. 2) discloses a method, comprising processing the modulus value and the shifted result using bit-by-bit subtraction to determine a subtracted result. The method further comprising determining a next working value from among a group consisting of the shifted result and the subtracted result by comparing the subtracted result to zero. The method further comprising storing the shifted and subtracted results in separate memories (col. 3, lines 41-55; col. 4, lines 39-50).

As to claims 10-12, method claims 10-12 correspond to apparatus claims 17-20; therefore, they are analyzed as previously discussed in claims 17-20 above.

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO-892

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C. 20231

or faxed to: (703) 872-9306 for all formal communications.

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Fourth Floor (Receptionist).

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fritz Alphonse, whose telephone number is (571) 272-3813. The examiner can normally be reached on M-F, 8:30-6:00, Alt. Mondays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert De Cady, can be reached at (571) 272-3819.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

Information regarding the status of an application may also be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Fritz Alphonse

Art Unit 2133

February 3, 2007

GUY LAMARRE
PRIMARY EXAMINER